Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claims 1–27 (CANCELED)

28 (AMENDED). A network based web content identification and control system ~~especially~~ for wide area networks, like the Internet, comprising:

~~client computer(s), which are any computers in the network;~~

~~examiner host computer(s), which are any computers in the network chosen for that purpose, and which each examine web content remotely by processing tiny sized delivered identifications of said web content locally;~~

~~wherein identification(s) of web content is delivered to an examiner host computer either before, during or after a client computer receives said web content from the network;~~

~~wherein said examiner host computer compares each of said delivered identification(s) to stored identifications of web content, and on the basis of the results of said comparison either:~~

- ~~(a) it is performed safety or preventive measures,~~
- ~~(b) and / or, said client computer and / or the user of said client computer is informed about the results of said comparison,~~
- ~~(c) or, no specific actions are performed;~~

~~wherein said web content comprises files, web pages, e-mail messages, e-mail message attachments or any data which a client computer can acquire from the network.~~

client computer(s), which are any computers in the network;

examiner host computer(s), which are remote third-party computers in the network;

performing an on-demand remote identity check on a specially established tiny-sized independent identification of the web content, what is used as a preferred method of processing rather than processing said web content as such;

wherein said identification is a data object which is based on certain property(ies) of said web content so that a unique representation of the identity of said web content is established;

wherein said identity check is performed by an examiner host in response to a remote service request;

wherein said identification is delivered without said web content for said identity check, in response to a client direct request to receive said web content from the network;

wherein the examiner host returns the results of said identity check as a feedback, and on the basis of said results:

(a) it is performed safety or preventive measures,

(b) and / or, it is informed said client,

(c) or, no specific actions are performed;

wherein the web content comprises file(s), web page(s), e-mail message(s), e-mail message attachment(s) or any data which a client can acquire from the network.

29 (AMENDED). A network based web content identification and control system according to claim 28, comprising:

~~wherein a said stored identification either:~~

~~(a) belongs to a specific web content,~~

~~(b) is an identification filter,~~

~~(c) or, partly belongs to a specific web content, and partly is an identification filter.~~

wherein said identity check comprises the examiner host comparing the delivered identification to stored identifications of web content.

Claim 30 (CANCELED)

31 (AMENDED). A network based web content identification and control system according to ~~claim 28~~ claim 29, comprising:

wherein [[a]] said delivered identification consists of file identification information and / or data identification information;

wherein a said stored identification consists of file identification information and / or data identification information;

wherein said file identification information comprises one or more of the following properties of the web content:

(a) source URL-address or other type of address,
(b) source computer URL-address or other type of address,
(c) name,
(d) type,
(e) content type,
(f) size,
(g) creation date,
(h) version number,
(i) publisher,
(j) authentication certificate,
(k) or, other properties;

wherein said data identification information comprises:

(a) a check-sum or any identification value based upon the data of the web content,

(b) and / or, a data sample picked according to a certain pattern, algorithm or other rule from the web content.

Claim 32 (CANCELED)

33 (AMENDED). A network based web content identification and control system according to ~~claim 32~~ claim 29, comprising:

wherein said stored identifications belong to known virus infected web content.

34 (PREVIOUSLY PRESENTED). A network based web content identification and control system according to claim 33, comprising:

wherein said safety measures include one or more of the following:

(a) preventing the download of the examined web content to the client computer,

(b) performing a virus scan on the examined web content in the client computer or in the examiner host computer,

(c) destroying the examined web content.

35 (AMENDED). A network based web content identification and control system according to claim 34, comprising:

wherein the examiner host ~~computer~~ calculates an estimate for the security threat level of the examined web content and informs it to the client ~~computer or the user of the client computer~~.

36 (AMENDED). A network based web content identification and control system according to claim 33, comprising:

intermediate computer(s), which are any computers in the network capable to intercept data which client computers receive from the network;

wherein said delivered identification[[~~(s)~~]] is delivered to the examiner host computer by a said intermediate computer.

37 (PREVIOUSLY PRESENTED). A network based web content identification and control system according to claim 36, comprising:

wherein said safety measures include one or more of the following:

(a) the intermediate computer preventing the download of the examined web content to the client computer,

(b) the intermediate computer performing a virus scan on the examined web content,

(c) the intermediate computer destroying the examined web content.

38 (PREVIOUSLY PRESENTED). A network based web content identification and control system according to claim 36, comprising:

wherein a said intermediate computer is:

(a) a server of the local area network,

(b) a server of the internet service provider,

(c) or, a network node computer.

39 (AMENDED). A network based web content identification and control system according to ~~claim 32~~ claim 29, comprising:

wherein said stored identifications belong to known non-wanted web content.

40 (PREVIOUSLY PRESENTED). A network based web content identification and control system according to claim 39, comprising:

wherein said preventive measures include preventing the download of the examined web content to the client computer, and / or destroying the examined web content.

41 (AMENDED). A network based web content identification and control system according to claim 39, comprising:

intermediate computer(s), which are any computers in the network capable to intercept data which client computers receive from the network;

wherein said delivered identification[[~~(s)~~]] is delivered to the examiner host computer by a said intermediate computer.

42 (PREVIOUSLY PRESENTED). A network based web content identification and control system according to claim 41, comprising:

wherein said preventive measures include the intermediate computer preventing the download of the examined web content to the client computer, and / or the intermediate computer destroying the examined web content.

43 (PREVIOUSLY PRESENTED). A network based web content identification and control system according to claim 41, comprising:

wherein a said intermediate computer is:

(a) a server of the local area network,

(b) a server of the internet service provider,

(c) or, a network node computer.

44 (PREVIOUSLY PRESENTED). A network based web content identification and control system according to claim 28, comprising:

wherein said client computers are host computers into which data is uploaded.

45 (AMENDED). A network based download information system especially for wide area networks, like the Internet, comprising:

client computer(s);

~~a host computer which keeps database of the identifications of the web content which the client computers or the users of client computers have downloaded from the network;~~

~~wherein said host computer retains client-specific information about one or more of the following:~~

~~(a) old and / or newly detected virus infections,~~

~~(b) old and / or newly detected security threats,~~

~~(c) old and / or newly determined security risk ratings,~~

~~(d) personal download statistics,~~
~~for said downloaded web content;~~

~~wherein the host computer informs / alerts the respective client computer and / or the user of said client computer, when said host computer retained client-specific information changes in certain way;~~

~~wherein a client computer and / or the user of said client computer is optionally able to access said host computer retained client-specific information;~~

~~wherein said web content comprises files or any data which a client computer can acquire from the network.~~

a register host computer which keeps for each client a client-specific download details register about the web content which the client has acquired from the network;

on the basis of a reiterated updated security check on a same web content which download details has been stored earlier in said register, the register host revising the security risk status for said web content;

wherein the web content comprises files or any data which a client can acquire from the network.

46 (AMENDED). A network based download information system according to claim 45, comprising:

wherein the pertinent client(s) is informed about said revised security risk status;

wherein the client ~~computer~~ destroys the host ~~computer~~ appointed harmful web content and / or performs a virus scan.

47 (NEW). A network based web content identification and control system according to claim 29, comprising:

wherein said safety or preventive measures are performed when said comparison yields a confirmed match.

48 (NEW). A network based web content identification and control system according to claim 47, comprising:

wherein if said comparison does not yield a definite match, then a close enough resemblance of the delivered identification to any of the stored identification(s) is deemed to be a confirmed match.

49 (NEW). A network based web content identification and control system for wide area networks, like the Internet, comprising:

client computer(s), which are any computers in the network;

examiner host computer(s), which are remote third-party computers in the network;

a client creating an ad-hoc independent identification for a web content by selectively extracting data item(s) from said web content or by generating signature(s) on the basis of selected data of said web content;

the client delivering said identification without said web content to an examiner host which performs in response to the client service request an on-demand analysis for said identification;

on the basis of said analysis, the examiner host determining whether the web content to which said identification belongs is:

(a) a security threat or not,

(b) or, non-wanted or not;

the examiner host returning feedback to the client, depending on the results of said analysis;

wherein the web content comprises file(s), web page(s), e-mail message(s), e-mail message attachment(s) or any data which a client can acquire from the network.

50 (NEW). A network based web access control method for wide area networks, like the Internet, comprising:

a client preparing to access a web-address to receive web content from the network;

the client creating an ad-hoc independent identification which contains at least:

(a) said web-address,

(b) or, a part of said web-address which identifies the pertinent host;

the client delivering said identification to a remote third-party examiner host which performs in response to the client service request an on-demand identity check for said identification;

on the basis of said identity check, the examiner host determining whether the entity to which said identification belongs is:

(a) a security threat or not,

(b) or, non-wanted or not;

the examiner host providing feedback to the client, depending on the results of said identity check;

wherein said web-address is a URL-address or other type of address.

51 (NEW). A network based web access control method according to claim 50, comprising:

preventing client access to the web content under said web-address if the examiner host determines said entity to be a security threat or non-wanted.

52 (NEW). A network based web access control method according to claim 50, comprising:

an intermediate computer creating and delivering said identification on behalf of the client, and receiving feedback from the examiner host on behalf of the client;

wherein the intermediate computer is any computer in the network capable to intercept data which the client receives from the network.

53 (NEW). A network based web access control method according to claim 52, comprising:

the intermediate computer:

(a) informing the client,

(b) and / or, preventing client access to the web content under said web-address,

if the examiner host determines said entity to be a security threat or non-wanted.

54 (NEW). A network based web content identification method for wide area networks, like the Internet, comprising:

in response to a client requesting to receive web content from the network, creating for remote delivery a tiny-sized ad-hoc independent identification for said web content;

wherein said identification is a data object which is based on certain property(ies) of said web content so that a unique representation of the identity of said web content is established;

delivering said identification without said web content to a remote third-party examiner host which performs in response to the service request an on-demand analysis for said identification;

the creation and delivery of said identification being performed by the client, or by an intermediate computer which is capable to intercept data which the client receives from the network;

the examiner host returning feedback on the basis of said analysis;

wherein the web content comprises file(s), web page(s), e-mail message(s), e-mail message attachment(s) or any data which a client can acquire from the network.